Amendments to the Claims:
Re-write the claims as set forth below. This listing of claims will replace all prior versions and listings, of claims in the application:

Listing of Claims:

1. – 5. (Canceled)

6. (Currently amended) A method for providing user authentication comprising:

receiving, from a first [[unit]]device, user identification data by an authentication [[unit]]device;

using, by the authentication device, the user identification data sent by the first [[unit]]device to determine which destination [[unit]]device, other than the first [[unit]]device, will receive an authentication code to be used to authenticate the user;

sending the authentication code to the determined destination [[unit]]device based on the user identification data;

receiving a returned authentication code back after sending the authentication code; and

authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

7. (Currently amended) The method of claim 6 including the step of generating the authentication code on a per authentication session basis and sending the authentication code to the determined destination [[unit]]device in response to the generated authentication code.

8. (Currently amended) The method of claim 6 including the step of maintaining per user destination [[unit]]device data including at least one destination [[unit]]device

identifier per user and wherein the step of using the user identification data to determine which destination [[unit]]device, other than the first [[unit]]device, will receive the authentication code includes sending the authentication code to the determined destination [[unit]]device based on the stored per user destination [[unit]]device identifier.

9. (Currently amended) The method of claim 6 wherein the returned authentication code is digitally signed and including the step of verifying, by the authenticating [[unit]]device, the digitally signed authentication code as part of the step of authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

10. (Currently amended) A method for providing user authentication comprising:

sending primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication [[unit]]device during a session;

using the primary authentication information to determine which destination [[unit]]device will receive an authentication code as secondary authentication information via a wireless back channel to be used to authenticate the user wherein the wireless back channel is an alternate channel to the primary wireless channel;

sending the authentication code on the wireless back channel to the destination [[unit]]device based on the primary authentication information during the same session;

returning the authentication code on the wireless primary channel to the authentication [[unit]]device during the same session; and

authenticating the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

11. (Original) The method of claim 10 including the steps of generating and sending the authentication code on a per authentication session basis.

12. (Currently amended) The method of claim 10 including the step of maintaining per user destination [[unit]]device data including at least one destination [[unit]]device identifier per user and wherein the step of using the primary authentication information to determine which destination [[unit]]device will receive the authentication code includes sending the authentication code to the destination [[unit]]device based on the stored per user destination [[unit]]device identifier.

13. (Currently amended) The method of claim 10 including the step of receiving user input in response to the step of sending the authentication code and waiting to return the authentication code to the authentication [[unit]]device until receipt of the user input.

14. (Currently amended) The method of claim 10 including the steps of:

prior to returning the authentication code to the authentication [[unit]]device, digitally signing, by the first [[unit]]device, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination [[unit]]device; and

verifying the digitally signed authentication code as part of authenticating the user.

15. (Currently amended) The method of claim 10 including the step of sending the authentication code on the wireless back channel to the destination [[unit]]device using at least one of a short message session (SMS) channel, a paging channel and a control channel.

16. (Original) The method of claim 10 including the step of: validating the primary authentication information.

17. (Currently amended) A storage medium comprising:

memory containing executable instructions that when executed by one or more processors, causes the one or more processors to:

receive, from a first [[unit]]device, user identification data by an authentication [[unit]]device;

use the user identification data to determine which destination [[unit]]device, other than the first [[unit]]device, will receive an authentication code to be used to authenticate the user;

send the authentication code to the determined destination [[unit]]device based on the user identification data;

receive a returned authentication code back after sending the authentication code; and

authenticate the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

18. (Currently amended) The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to generate the authentication code on a per authentication session basis and send

the authentication code to the determined destination [[unit]]device in response to the generated authentication code.

19. (Currently amended) The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to maintain per user destination [[unit]]device data including at least one destination [[unit]]device identifier per user and send the authentication code to the determined destination [[unit]]device based on the stored per user destination [[unit]]device identifier.

20. (Currently amended) The storage medium of claim 17 including memory containing instructions that when executed by one or more processors, causes the one or more processors to digitally sign the returned authentication code and verify, by the authenticating [[unit]]device, the digitally signed authentication code as part of authenticating the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

21. (Currently amended) A storage medium comprising:

memory containing executable instructions that when executed by one or more processors associated with one or more devices, causes the one or more processors to:

send primary authentication information on a primary wireless channel by a primary authentication information provider to an authentication [[unit]]device during a session;

use the primary authentication information to determine which destination [[unit]]device will receive an authentication code as secondary authentication information

via a wireless back channel to be used to authenticate the user wherein the wireless back channel is an alternate channel to the primary wireless channel;

send the authentication code on the wireless back channel to the destination [[unit]]device based on the primary authentication information during the same session;

return the authentication code on the wireless primary channel to the authentication [[unit]]device during the same session; and

authenticate the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

22. (Original) The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to generate and send the authentication code on a per authentication session basis.

23. (Currently amended) The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to maintain per user destination [[unit]]device data including at least one destination [[unit]]device identifier per user and send the authentication code to the destination [[unit]]device based on the stored per user destination [[unit]]device identifier.

24. (Currently amended) The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to receive user input in response to the step of sending the authentication

code and wait to return the authentication code to the authentication [[unit]]device until receipt of the user input.

25. (Currently amended) The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to:

prior to returning the authentication code to the authentication [[unit]]device, digitally signing, by the first [[unit]]device, the returned authentication code to produce a digitally signed authentication code that was received from the determined destination [[unit]]device; and

verifying the digitally signed authentication code as part of authenticating the user.

26. (Currently amended) The storage medium of claim 21 containing memory having executable instructions that when executed by one or more processors, causes the one or more processors to send the authentication code on the wireless back channel to the destination [[unit]]device using at least one of a short message session (SMS) channel, a paging channel and a control channel.

27. (Currently amended) A system for providing user authentication comprising:

a first [[unit]]device;

a second [[unit]]device operatively coupleable to the first [[unit]]device via a primary wireless channel and operatively coupleable to an authenticator; and

a third [[unit]]device, operatively coupleable to the second [[unit]]device via a wireless back channel,

the first [[unit]]device operative to send primary authentication information via the primary channel during a session to the second [[unit]]device;

the authenticator operative to use the primary authentication information to determine which destination [[unit]]device, other than the first [[unit]]device, will receive an authentication code as secondary authentication information via the wireless back channel and wherein the destination [[unit]]device is the third [[unit]]device;

the second [[unit]]device operative to the send the authentication code on the wireless back channel to the destination [[unit]]device based on the primary authentication information sent via the primary channel during the same session;

the first [[unit]]device operative to return the authentication code on the wireless primary channel to the second [[unit]]device during the same session; and

the authenticator operative to authenticate the user when the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel.

28. (Currently amended) The system of claim 27 wherein the authenticator maintains per user destination [[unit]]device data including at least one destination [[unit]]device identifier per user and sends the authentication code to the second [[unit]]device for transmission to the destination [[unit]]device based on the stored per user destination [[unit]]device identifier.

29. (Currently amended) The system of claim 27 wherein the first [[unit]]device includes an interface to receive user input in response to the sending of the authentication code and wherein the first [[unit]]device waits to return the authentication code for the authenticator until receipt of the user input.

30. (Currently amended) The system of claim 27 wherein the first [[unit]]device includes a cryptographic engine and prior to the first [[unit]]device returning the authentication code for the authenticator, digital signs the returned authentication code to produce a digitally signed authentication code that was received from the third [[unit]]device; and wherein the authenticator verifies the digitally signed authentication code as part of authenticating the user.

31. (Currently amended) The system of claim 27 wherein the second [[unit]]device [[send]]sends the authentication code on the wireless back channel to the third [[unit]]device using at least one of: a short message session (SMS) channel, a paging channel and a control channel.